# AUTOMATICALLY GENERATING VALID BEHAVIOR SPECIFICATIONS FOR INTRUSION DETECTION

## ABSTRACT

One embodiment of the present invention provides a system that automatically generates a valid behavior specification for use in an intrusion detection system for a computer system. The system operates by receiving an exemplary set of system calls that includes positive examples of valid system calls, and possibly negative examples of invalid system calls. The system automatically constructs the valid behavior specification from the exemplary set of system calls by selecting a set of rules covering valid system calls. This set of rules is selected to cover all positive examples in the exemplary set of system calls without covering negative examples. Moreover, the process of selecting a rule for the valid behavior specification involves using an objective function that seeks to maximize the number of positive examples covered by the rule while seeking to minimize the number of possible system calls covered by the rule. In one embodiment of the present invention, the system additionally monitors an executing program. During this monitoring process, the system receives a system call generated by the executing program. The system next determines whether the system call is covered by a rule from within the valid behavior specification. If not, the system generates and indication that the system call is invalid.

26